



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 15 July 2004

Current Nationwide
Threat Level is



[For info click here](http://www.whitehouse.gov/homeland)
www.whitehouse.gov/homeland

Daily Overview

- The Transportation Security Administration on Wednesday announced it will begin an operational test and evaluation of an explosives trace detection portal at a passenger security checkpoint at San Diego International Airport's Lindbergh Field. (See item [12](#))
- The Department of Homeland Security on Wednesday announced the broadening of its new initiative called the Regional Technology Integration to the Anaheim, CA, urban area. (See item [29](#))
- The Associated Press reports that a computer database of the largest downtown buildings in Minneapolis will soon enable city police officers and firefighters to get a computer printout of the layout of downtown buildings before they arrive at the scene of an emergency. (See item [37](#))

DHS/IAIP Update Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *July 14, Associated Press* — **Power out in wake of storms.** Thousands of homes and businesses had no electricity Wednesday, July 14, in the path of a long line of thunderstorms that stretched from Tennessee to the Great Lakes. Wind gusted to 80 mph in Kentucky and Tennessee on Tuesday, July 13, and hail stones as big as softballs were reported in parts of Illinois, the National Weather Service said. **Utilities around Kentucky reported about**

254,000 homes and businesses lost power during the storms, including 115,000 in the Louisville metropolitan area. Chip Keeling, a spokesperson for Louisville Gas & Electric, said power had been restored to about 40,000 customers by Wednesday morning but some might remain in the dark for an extended period. About 60,000 customers were blacked out in central Tennessee, but service had been restored to about half of them by dawn Wednesday, Nashville Electric Service reported. Some 51,000 customers were still without power Wednesday morning in Indiana, down from a high of up to 136,000 during the storms, said Cinergy-PSI utility spokesperson Angeline Protogere. Some might have to wait until Thursday for the lights to go on again, she said. Utilities said at least 10,000 customers lost power in Michigan.

Source: <http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2004/07/14/national1115EDT0562.DTL>

2. *July 14, Associated Press* — **BPA maintenance increased to ensure steady power flow.** The Bonneville Power Administration (BPA) is taking steps to prevent a major blackout like the one that happened in the Northeast last summer or the one that hit the West Coast in 1996. In both cases, overloaded lines sagged into trees on a hot day, triggering a cascade of power failures over thousands of square miles. The aim of the BPA, which markets electricity generated at 31 federal dams and one nuclear-power plant, is to ensure the steady flow of power from generators along the west coast. **For the first time since 1987, the agency is adding power lines to the 15,000-mile Northwest grid, which crosses Oregon, Washington, Idaho and western Montana.** At the same time, BPA has increased its tree-trimming budget to \$10.1 million a year. **The agency also has spent \$93 million on three projects to update grid-operating systems in Oregon and Washington.** BPA is asking utility experts and conservationists for ideas on how to defer the construction of new lines, at a cost of about \$1.1 million a mile, while preventing shortages during peak periods. BPA owns 75 percent of the region's power lines.

Source: http://seattletimes.nwsources.com/html/localnews/2001979024_grid14m.html

3. *July 14, Oil and Gas Journal* — **Experts debate government role in averting U.S. oil worker shortages.** Officials from oil-producing states saw a slight increase last year in the number of students entering the U.S. oil and gas business, but the pace was not enough to stem what is expected to be a growing tide of retirements within the industry, North Dakota Governor John Hoeven told the House Subcommittee on Energy and Minerals Resources Thursday, July 8. Helping to avert a looming labor shortage will take a concerted effort by both industry and government, according to some witnesses. **"There is a growing shortage of qualified workers in the industry today and that dilemma will require the combined efforts of the public and the private sectors to address,"** Hoeven said on behalf of the Interstate Oil & Gas Compact Commission (IOGCC). **"Without solving this problem, any plan to increase domestic supplies of natural gas and oil will be difficult to implement,"** he said. The IOGCC blamed part of the problem on industry itself, saying companies need to sell themselves better. Hoeven and other witnesses also cited a landmark 1999 National Petroleum Council study that predicted more than 40% of the industry's scientific workforce would retire during this decade.

Source: http://ogi.pennnet.com/articles/web_article_display.cfm?ARTICLE_CATEGORY=GenIn&ARTICLE_ID=208194

Chemical Industry and Hazardous Materials Sector

4. *July 14, American City Business Journals* — **Peach State Labs grows with acquisition.** Peach State Labs, a specialty polymer chemical company from Rome, GA, has bought Dalton, GA-based American Emulsions Inc., a subsidiary of RPM International Inc. The acquisition gives Peach State Labs expanded production capabilities. "Our acquisition of American Emulsions reinforces Peach State Labs commitment to becoming one of the world's premier specialty polymer chemical companies," said Rick Sargent, president and CEO of Peach State Labs. "Over the past few years we've seen increased demand for our specialty polymer chemicals. The acquisition of American Emulsions' production facility will give Peach State Labs expanded production capabilities to meet customer demand."

Source: <http://atlanta.bizjournals.com/atlanta/stories/2004/07/12/daily15.html>

Defense Industrial Base Sector

5. *July 14, Associated Press* — **U.S. Army shows off latest in mobile care.** U.S. Army researchers and contractors last week displayed equipment designed to be lighter, tougher and more efficient than those now in use. At Fort Detrick, MD, home of the U.S. Army Medical Research and Materiel Command, a private vendor demonstrated its 21st Century Military Hospital System, a system in which tents are joined and ready for use in 15 minutes, supported by inflatable beams and equipped with a generator for heating, cooling, lighting and air filtration. Researchers at Fort Detrick are refining sensors that can transmit a soldier's vital signs wirelessly to a medic's hand-held receiver. **Colonel Beau Freund, deputy commander of the U.S. Army Research Institute of Environmental Medicine, said about 20 percent of medics killed in action die trying to reach soldiers who are already dead, and this system could help reduce that statistic.** Army researchers also are working to improve bandages and tourniquets, fluids to prevent shock, pain control and containers for keeping blood cool. Half of battlefield deaths are from blood loss, said Major Bob Wildzunas, director of research at the U.S. Army Institute of Surgical Research.

Source: http://www.herald-mail.com/?module=displaystory&story_id=83568&format=html

Banking and Finance Sector

6. *July 14, Washington Post* — **Obstacles block tracking of terror funding.** President Bush and his top officials have repeatedly said that detecting and interrupting the flow of funds to illicit activities is a vital component in the battle against terrorism. Getting front-line financial institutions to alert officials to suspicious money movements is one key to that effort. Critics see recent industry reporting lapses as evidence of troubling gaps in the monitoring machinery. **Critics in Congress say that strides have been made in the past three years to interrupt funding flows and that coordination among agencies has improved. However, because**

underground groups are finding ever more evasive ways to maneuver and to disguise assets, the problem remains critical. Monitoring efforts have been hindered by a historic reluctance by bank regulators to become law enforcement agents; gaps in top Department of Treasury; fragmented state and federal bank regulation; and the inherent difficulty of writing rules that don't overburden an already highly regulated banking industry and make doing business with foreigners too cumbersome.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A48391-2004Jul 13.html>

7. *July 14, Finextra Research* — **Phishing financial burden is significant. Financial institutions stand to lose an estimated \$400 million in fraud losses resulting from phishing attacks in 2004**, according to research by Financial Insights. According to the research, the number of unique phishing attacks reported to the Anti-Phishing Working Group increased from just 19 in November 2003 to 1197 in May 2004. Financial Insights says in addition to the management of identity theft cases, **institutions targeted by phishers are also incurring additional organizational costs and are suffering from an erosion in customer trust.**

Sophie Louvel, research analyst and author of the report, says most of the anti-phishing systems currently available are focused on detection of phishing attacks, but it will require significant and widespread security enhancements to e-mail technology to curb these attacks.

Source: <http://www.finextra.com/fullstory.asp?id=12173>

8. *July 14, Boston Globe* — **Firms hit hard by identity theft. Government agencies and private corporations are vulnerable to identity theft, and they often suffer greater losses than the client whose personal information was stolen**, authorities said Tuesday, July 13. **When credit card or bank account numbers are stolen from corporations such as credit agencies, it is often the institutions, and not private citizens, who are hit the hardest**, said Ken Jones, inspector in charge for the regional Postal Inspection Service in Boston, MA. While it's difficult to pin down an exact dollar amount lost when identity thieves strike such institutions, Jones said 20 cases that have been proposed for federal prosecution involve \$300,000 to \$1 million in losses each. From October 1 to June 30, the Massachusetts Identity Theft/Financial Crimes Task Force made 262 arrests in New England in connection with identity theft. Kevin Kiley of the Massachusetts Bankers Association said his group and the Massachusetts Chiefs of Police plan to unveil an identity-theft protocol in the fall that would improve police training and allow citizens to go directly to police departments across the state to report identity theft. The information could then be fed directly to the task force.

Source: http://www.boston.com/business/technology/articles/2004/07/14/firms_hit_hard_by_identity_theft/

9. *July 13, SecurityFocus* — **Companies adapt to a zero day world.** Zero day exploits are here. Case in point, the June 25th Russian attacks that turned IIS servers into delivery platforms for identity-thieving Trojan keystroke loggers. The attacks relied on two vulnerabilities in Internet Explorer that security researchers discovered for the first time weeks earlier on a malicious adware-implanting Website. At the time of the attack, no patch was available. ISPs were able to quickly contain the threat by shutting down traffic to the Russian host serving up the malware. However, the episode proved that the zero day concern is more than hyperbole. As the window shrinks between the discovery of vulnerabilities and the exploits that follow them, **security patching — once an obscure and neglected chore — is beginning to take on a more urgent role in some corners of the business world, say analysts and IT managers.**

Leading the way are organizations with mission-critical technology -- chiefly finance agencies -- who've managed to reduce critical security patch times from weeks to just days. The key, they say, is that they've moved patch management from their small security organizations into their network infrastructure management.

Source: <http://www.securityfocus.com/news/9100>

[\[Return to top\]](#)

Transportation Sector

10. *July 14, Omaha World-Herald (NE)* — **Freight capacity choking on demand: the coming peak season for shipping raises concerns.** The nation's transportation network--especially rails, highways and international ports--is straining under shipping demand that is fast outpacing the network's capacity. **By 2020, total freight tonnage moved in the United States is expected to increase by 67 percent, according to a U.S. Chamber of Commerce report. The capacity crunch has become more apparent by prolonged congestion and service delays on the nation's largest railroad, Omaha-based Union Pacific, as well as one of its counterparts in the east, CSX Transportation.** Now shippers and government and corporate officials are bracing for the start of peak shipping season. The three transportation modes also have faced manpower shortages, further cramping capacity. Railroads began a hiring spree after many longtime conductors and engineers took advantage of a recently enhanced federal retirement program, trucking companies saw productivity drop after new federal hours-of-service regulations went into effect in January, and the nation's ports, especially in the west, are growing more congested as they handle larger ships, new regulations, and increasing amounts of intermodal traffic.

Source: http://cnni.wyellowbrix.com/pages/cnni/Story.nsp?story_id=53988009&ID=cnniw&scategory=Transportation%3ARail&

11. *July 14, Associated Press* — **Power outage delays flights in Minnesota.** A power outage at a Northwest Airlines facility Wednesday, July 14, caused dozens of cancellations and delays for its departing flights nationwide. **Northwest spokesperson Mary Stanik said there was a power failure about 8:15 a.m. at a facility in suburban Eagan, MN, near Minneapolis-St. Paul International Airport.** Northwest told the Federal Aviation Administration (FAA) that the problem had been fixed and flights were expected to return to normal during the day, FAA spokeswoman Elizabeth Isham Cory said. In all, 60 Northwest flights were canceled, plus 150 flights on its subsidiary carriers, Stanik said. The outage caused tie-ups on the ground because landing flights could not go to their gates until the outbound Northwest flights could leave.

Source: http://seattlepi.nwsourc.com/national/apus_story.asp?category=1110&slug=Airport%20Delays

12. *July 14, Transportation Security Administration* — **San Diego International Airport is TSA test bed for explosives trace detection portals.** The Transportation Security Administration (TSA) Wednesday, July 14, announced it will begin an operational test and evaluation of an explosives trace detection portal at a passenger security checkpoint at San Diego International Airport's Lindbergh Field in California. In June, TSA began testing at T.F. Green State Airport, Providence, RI, and Greater Rochester International Airport, NY. In the next few weeks, machines will be introduced to air travelers at Tampa International

Airport, NY, and Gulfport–Biloxi International Airport, MS. The explosive trace detection portal, the GE EntryScan3, is designed to analyze air for traces of explosive material and will be evaluated for effectiveness in the airport environment. The tests will be conducted for 30 to 45 days at each airport.

Source: http://www.tsa.gov/public/display?theme=44&content=090005198_00b827d

13. *July 13, GAO* — **GAO–04–795: Border Security: Additional Actions Needed to Eliminate Weaknesses in the Visa Revocation Process(Report).** The National Strategy for Homeland Security calls for preventing foreign terrorists from entering our country and using all legal means to identify; halt; and where appropriate, prosecute or bring immigration or other civil charges against terrorists in the United States. The Government Accountability Office (GAO) reported in June 2003 that the visa revocation process needed to be strengthened as an antiterrorism tool and recommended that the Department of Homeland Security (DHS), in conjunction with the Departments of State (State) and Justice, develop specific policies and procedures to ensure that appropriate agencies are notified of revocations based on terrorism grounds and take proper actions. **To improve the visa revocation process as an antiterrorism tool, GAO recommends that the Secretaries of DHS and State jointly (1) develop a written governmentwide policy that clearly defines roles and responsibilities and sets performance standards and (2) address outstanding legal and policy issues in this area or provide Congress with specific actions it could take to resolve them.** Highlights:

<http://www.gao.gov/highlights/d04795high.pdf>

Source: <http://www.gao.gov/new.items/d04795.pdf>

[[Return to top](#)]

Postal and Shipping Sector

14. *July 14, Times Picayune (LA)* — **Meraux post office gets the all-clear. The Meraux, LA, post office is scheduled to reopen Wednesday, July 14, now that the state Department of Health and Hospitals (DHH) has given the all-clear after a Monday, July 12, anthrax hoax.** The incident began Monday, July 12, about 6:30 a.m. when a customer found a small plastic bag containing white powder on the lobby floor of the Meraux post office. The customer called the Sheriff's Office, and deputies secured the perimeter of the building. Investigators from the St. Bernard Parish Fire Department, the Environmental Protection Agency (EPA), the FBI and the U.S. Postal Inspection Service soon joined the investigation. Investigators said they don't take such threats lightly. "State epidemiologists have come to the conclusion that it was not anthrax or any other bio-terror agent," said Kristen Meyer, a spokesperson for the DHH.

Source: http://www.nola.com/news/t-p/index.ssf?/base/news-1/10897936_41199110.xml

[[Return to top](#)]

Agriculture Sector

15. *July 14, Reuters* — **Eight Thai provinces hit by new bird flu outbreak. Thailand now has new outbreaks of the deadly bird flu which ravaged Asian flocks early this year in eight**

provinces and it may have returned to Bangkok, a senior Agriculture Ministry official said on Wednesday, July 14. "Bird flu is confirmed in two farms in Sukothai and Chiang Rai provinces," Yukol Limlaemthong, head of the ministry's Livestock Department, told reporters. That confirmation meant new outbreaks had now been reported in eight of the country's 76 provinces. "We have sent samples from some farms in Bangkok for lab testing and the results would be known in a few days," Yukol said. **More than 25,000 fowl had been culled as a result of the latest outbreaks, officials said, and Prime Minister Thaksin Shinawatra said any poultry showing signs of the disease which killed 16 Vietnamese and 8 Thais earlier this year would follow.** Last week, outbreaks of the H5N1 bird flu virus were confirmed in two central provinces, ending Thai hopes that the avian flu outbreak which ravaged poultry farms across Asia earlier this year had been eradicated.

Source: <http://www.alertnet.org/thenews/newsdesk/BKK209641.htm>

16. *July 14, ABC Australia* — **Vietnam confirms return of lethal strain of bird flu.** Vietnam has confirmed that fresh outbreaks of bird flu were caused by the lethal strain of the disease which killed 16 people in the country earlier this year. A spokesman for Vietnam's Agriculture ministry says tests carried out by experts in Ho Chi Minh City in the country's south, show the presence of the H5N1 virus. **Vietnam's state-run media reports that bird flu outbreaks have occurred in 14 districts in seven southern provinces and cities since mid April.** The World Health Organization has warned that it could take months, probably years, to eliminate the H5N1 virus from the environment. More than 44 million poultry have died or were slaughtered across Vietnam as a result of the bird flu.

Source: http://abcasiapacific.com/news/stories/asiapacific_stories_1_153388.htm

17. *July 14, Nebraska Ag Connection* — **Aphids spotted in Nebraska. Soybean aphids are showing up in several Nebraska counties so growers need to check their fields now for the relatively new pests, a University of Nebraska entomologist said.** As of Tuesday, July 13, aphids had been spotted in Lancaster, Saunders, Butler, Pierce, Dixon, and Buffalo counties. Tom Hunt, a University Institute of Agriculture and Natural Resources entomologist, said hotter temperatures settling into the state should slow down the aphids. In most cases, he said, aphid damage is minimal to soybeans at this time, and most reports so far have cited only a few aphids per field. However, the aphids are expected to occur in all soybean production regions of Nebraska this summer. They can reproduce rapidly when temperatures are in the 70s and 80s. Soybean aphids can transmit viral diseases such as alfalfa mosaic, soybean mosaic, bean yellow mosaic, peanut mottle, peanut smut, and peanut stripe. Severe infestations can reduce yields 20 percent to 30 percent, Hunt said.

Source: <http://www.nebraskaagconnection.com/story-state.cfm?Id=390&y r=2004>

18. *July 14, Pantagraph.com* — **Disease shows up in corn. Central Illinois corn growers may be facing an unprecedented outbreak of gray leaf spot in terms of earliness of infection and potential for large yield losses.** Continual leaf wetness and high humidity appear to have fostered the disease. Losses can range from 5 bushels to 40 bushels per acre. Corn growers last dealt with the fungal disease in 2000 and 1996 when the disease hit late in the season. The disease typically occurs in late July or August. "This is unprecedented in that it's occurring early. Plants have stayed wet a long time," said Scott Schertz, owner of Schertz Aerial Service at Hudson. "It will greatly affect cob fill. The upper leaves give energy for filling. In three weeks, untreated fields will look like they're dying prematurely. This is about keeping the plant

alive." Schertz has sprayed fields in McLean and southern Livingston counties. He and others cautioned that not every field is infected.

Source: http://www.pantagraph.com/stories/071404/bus_20040714004.sht ml

[[Return to top](#)]

Food Sector

19. *July 13, Reuters* — USDA probe finds holes in mad cow testing. A government investigation on Tuesday, July 13, gave the U.S. Department of Agriculture (USDA) poor marks in testing cattle for mad cow disease, saying the agency was neglecting to test the majority of cattle most at risk. "The problems identified during our review, if not corrected, may ... reduce the credibility of any assertion regarding the prevalence of BSE (bovine spongiform encephalopathy) in the U.S.," said the USDA's Office of Inspector General. The report said the USDA was not testing adult cattle that died on the farm and had failed to test hundreds of cattle condemned due to possible central nervous system disorder — a symptom of mad cow disease and many other diseases. "A process for obtaining samples from animals that died on the farm has not been developed," the report said. Ron DeHaven, head of USDA's Animal and Plant Health Inspection Service, said 70 percent of its mad cow tests last month came from dead cattle arriving at the slaughter plant. "Nothing in the report would cause us to change the focus of the program," DeHaven said in an interview. The USDA emphasized that the internal investigation took place months before the enhanced surveillance program started in June.

Source: <http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=5660795>

20. *July 13, CIDRAP News* — Canada to boost feed restrictions to prevent mad cow. The Canadian government has announced it will ban high-risk cattle parts from all animal feeds, including pet food, as a further step to prevent the spread of mad cow disease — also known as bovine spongiform encephalopathy (BSE). The Canadian Food Inspection Agency (CFIA) did not say when the restriction would take effect. The Canadian action pertains to specified risk materials (SRMs) — tissues that, in infected cattle, harbor the abnormal prion proteins that cause BSE. SRMs generally include the skull, brain, spinal cord, eyes, tonsils, vertebral column, small intestine, and certain nerve bundles. Both Canada and the United States require the removal of SRMs from carcasses intended for human consumption. **The purpose of banning SRMs from all animal feeds is to reduce the risk of cross-contamination in feed manufacturing, whereby SRMs used in chicken or pig feed could enter cattle feed if both kinds of feed were made with the same equipment.** A ban would also limit the risk from giving cattle the wrong kind of feed.

Source: http://www.cidrap.umn.edu/cidrap/content/hot/bse/news/july13_04canada.html

[[Return to top](#)]

Water Sector

21. *July 14, Star-Ledger (NJ)* — Senior center fights Legionnaires' disease. Health officials in Paterson, NJ, continued to advise residents at a senior housing center Tuesday, July 13,

not to drink the tap water or to use the showers after two people were stricken by Legionnaires' disease, one of them fatally. Both victims lived in the Nathan Barnert Senior Housing Center, owned by the city's housing authority. No other residents of the 96-unit building have exhibited symptoms of the illness, according to Stephen Summers, a spokesman for the Passaic County Department of Health. He said officials from the Paterson Division of Health, along with county and state health officials, are monitoring the situation. Paterson Housing Authority officials shut off the hot water Saturday after preliminary lab results from the state Department of Health detected bacteria in the water supply. **The building's water system is being remediated by an outside firm, and the 117 residents are being provided with bottled water for drinking, washing, and bathing until the system is cleaned.**

Source: <http://www.nj.com/news/ledger/jersey/index.ssf?/base/news-6/1089791509222830.xml>

- 22. July 14, *Engineering News Record* — Long dry spell taxes utilities in the West. As drought grips the Western U.S., regional water agencies are gearing up for short-term and long-term measures to keep the water flowing. Agencies are planning major investments and seeking out innovative sources, like desalination and groundwater reclamation.** Facing a 75 percent decline in supplies from the Rio Grande River, El Paso, TX, implemented an emergency 77-day, eight million dollar project. The city installed three mobile skid-mounted reverse osmosis units to reclaim eight million gallons per day of brackish water from 11 defunct wellheads, says Craig Goehring, a project engineer. In another significant move, the San Diego, CA, Water Authority approved a \$1.8-billion master plan in late June. Highlights include a 50-million-gallon-per-day water treatment plant. In Orange, CA, construction is under way on the innovative \$487-million Groundwater Replenishment System, which will recharge groundwater with highly treated wastewater, providing supplies during droughts and recharging the saltwater intrusion barrier. **Drought relief is nowhere in sight, largely because of this year's drastically diminished western snowpack. Nature's cold storage system normally provides about 75 percent of the water supply in 11 states.**

Source: <http://www.enr.com/news/environment/archives/040719-1.asp>

[[Return to top](#)]

Public Health Sector

- 23. July 14, *Medical News Today* — West Nile virus trial. The National Institute of Allergy and Infectious Diseases (NIAID) has expanded its clinical trial of an experimental West Nile virus (WNV) treatment to about 60 sites throughout the U.S. and Canada. The multicenter trial, which opened at 36 sites last September, is expected to add about 24 new sites this summer.** The study is testing the safety and preliminary effectiveness of using a product containing West Nile infection-fighting proteins, or antibodies, to treat people whose infection has reached or threatens to reach the brain. "As West Nile virus disease continues to spread across our country, it is critical that we develop specific treatments for its most severe symptoms," says Anthony S. Fauci, NIAID director. "At present, clinicians have few options besides supportive care for treating people with West Nile illness. By expanding this study, we hope to accelerate NIAID's efforts to understand, develop treatments for and eventually prevent this disease." The main goal of this study, notes Walla Dempsey, who oversees NIAID's West Nile clinical trial contracts, is to assess the safety of a blood plasma-derived substance

containing West Nile antibodies when given intravenously to patients with West Nile infection. Secondly, she adds, the study seeks preliminary data about the treatment's effectiveness against encephalitis, a brain inflammation caused by the infection.

Source: <http://www.medicalnewstoday.com/medicalnews.php?newsid=10691>

24. *July 14, Associated Press* — **CDC ships chem-packs for preparation. The government is shipping stocks of antidotes against chemical weapons to states under a long-awaited program to boost response to a potential terrorist attack.** New York and Boston, sites of the upcoming political conventions, were among the first areas to receive the chem-packs. **Within two years, the Centers for Disease Control and Prevention (CDC) hopes to have the allotments dispersed to every state.** "It's a quick way for hospitals to know they'll have the antidotes they need," said Donna Knutson, CDC's deputy director of terrorism preparedness. The program was begun in part because there has been "an uneven level of protection across the country," added Steve Adams, deputy director of the Strategic National Stockpile Program. The National Pharmaceutical Stockpile contains drugs, vaccines, and other medical supplies in storage around the country, so that any U.S. city could receive an emergency shipment within 12 hours. That's probably plenty of time to react to an incubating infection like anthrax, but the ability to survive a chemical attack depends on immediate decontamination and rapid administration of appropriate antidotes. The chem-packs come with an assortment of antidotes to the many chemicals available to a terrorist. Some are in autoinjectors for use at the site of an attack, others packaged for emergency-room use.

Source: <http://apnews.myway.com/article/20040714/D83QAGH82.html>

25. *July 14, Oregonian* — **Scientists check the body's defenses for safer vaccines. Oregon scientists hope that aging monkeys and a modified smallpox vaccine can help explain a medical mystery: Why senior citizens and infants get sick so easily.** Weakened immune systems are a hallmark of both ends of life, contributing to disease and death in babies younger than a year and adults 60 and older. A new federal grant will give Oregon Health & Science University (OSHU) researchers \$10 million during five years to study why those immune changes happen. Scientists have "very fragmented" and "certainly incomplete" understanding of those reasons today, said lead researcher Janko Nikolich-Zugich, with OHSU's Vaccine and Gene Therapy Institute. **One goal is to make vaccines safer and better for the young, the old, and others with weakened immune systems.** Once scientists understand the defects that weaken aging immune systems, they can look for ways to overcome those defects, said Rebecca Fuldner, an administrator with the National Institute on Aging, which awarded OHSU the grant. "It's very difficult to immunize people of that age (older than 60) against a new pathogen the body has never seen before," she said. Fuldner said federal interest in protecting people with weakened immune systems is growing for several reasons: The U.S. population is aging. New diseases are emerging. And the country is planning for possible disease attacks by terrorists.

Source: <http://www.oregonlive.com/news/oregonian/index.ssf?/base/new/s/1089806600311330.xml>

26. *July 13, Australian Associated Press* — **Plants could vaccinate against malaria. Australian scientists have discovered that animals can develop immunity to the mosquito-borne disease by eating purified malaria proteins,** Monash University's Professor Ross Coppel said. "What we've shown is that you can actually vaccinate animals and protect them against malaria

by feeding them purified proteins," Coppel said. "What we now want to do is to make the source of proteins a plant that makes the malaria protein, rather than growing it in bacteria and purifying it, which adds a lot of expense when you do it on a large scale." **If Coppel's team achieves their aim, people will be able to vaccinate themselves against malaria by simply eating the plant.** "The theory is that once you eat it, the body recognises the foreign malaria protein and makes antibodies," he said. "That's something that's potentially a very cheap way of reaching a very large number of people in the developing world where the conventional injectable syringes have all the problems of keeping them cold, of using needles in places where there's often HIV and where they don't have much money to support those programs."

Source: <http://www.theage.com.au/articles/2004/07/13/1089694342376.html?oneclick=true>

27. *July 13, Cox News Service* — **Computer program tracks outbreaks.** Blue blips bloom on the computer screen, flowing across the map of metro Atlanta, GA, with the click of a mouse. Color surges through Newnan and Douglasville, Marietta and Dawsonville. It turns at Gainesville, blazing and fading through Lawrenceville, Tucker, and Decatur and settling downtown in an indigo glow. If the blue blips were real, they would display the path of an epidemic as it flared across the metro area. For now, they are a display of fictional data loaded as a test into computers at the Centers for Disease Control and Prevention (CDC). But they mark the achievement of a goal the CDC has pursued since before the 2001 anthrax alerts: using technology to detect the earliest indications of a bioterrorist attack. **The blips are the product of a project called BioSense, a massive computer program developed by the CDC and private designers that scans for anomalies in routinely compiled databases of symptoms, diagnoses, drug sales, and other health data.** Its earliest prototype began operating late last year, and the system now covers about 30 cities. **If successful, BioSense could solve an intractable problem in disease detection and biodefense: shortening the time lag between a patient's first flicker of symptoms and the realization by authorities that an epidemic has begun.**

Source: http://www.news-journal.com/news/content/shared/news/stories/0713_cdcbioterror.html:COXnetJSessionID=A115K91hdc6gNqWI18VWKvfokE7TCvnJywMg0ekFs2TY8ekAbG37!-697910054?urac=n&urvf=10898118979080.5962529056416612

[[Return to top](#)]

Government Sector

28. *July 15, National Journal* — **Officials discuss efforts to network crime, terrorism data.** The Department of Homeland Security (DHS) is working to connect its nationwide information network to existing law enforcement databases, an official told lawmakers Tuesday, July 13. DHS is working with the Justice Department to make the systems "fully compatible in the short term and [is] developing a common system for the future," Patrick Hughes, Homeland Security's assistant secretary for information analysis, told a House Government Reform subcommittee. DHS officials have yet to connect the network to the Law Enforcement Online (LEO) and the secure intranet of the Regional Information Sharing System (RISS). More than 30,000 law enforcement officers use LEO to disseminate and share criminal, cyber and terrorism intelligence across the secured RISS network. The department announced last week that it has connected to its information network law enforcement and operators of

critical infrastructures in all 50 states and more than 50 urban areas.

Source: http://www.govexec.com/story_page.cfm?articleid=28975&dcn=to daysnews

29. *July 14, Department of Homeland Security* — **Homeland Security launches regional technology integration initiative in California.** The Department of Homeland Security (DHS) on Wednesday, July 14, announced the broadening of its new initiative called the **Regional Technology Integration (RTI) to the Anaheim, CA, urban area.** RTI facilitates the transition of innovative technologies and organizational concepts to regional, state, and local jurisdictions. Through the program, managed by DHS's Science & Technology directorate, four urban areas across the country have been selected to be the initial pilot locations for this program. **The goal of the RTI initiative is to speed the successful transfer and integration of existing and advanced homeland security technology systems to local governments in order to improve their preparedness and response.** The program focuses on the prompt implementation of technologies for detection and response; the collaboration with end-users and other DHS programs; the integration of new technologies with the existing infrastructure, systems and concepts to reduce costs and assure sustainability; and measurable objectives and continuous evaluation to ease the utilization of lessons learned and best practices by other communities.

Source: <http://www.dhs.gov/dhspublic/display?content=3822>

30. *July 14, Department of Homeland Security* — **Homeland Security partners with state and locals to protect Democratic National Convention.** Secretary Tom Ridge met Wednesday, July 14, with officials in Boston, MA, to review security measures for the Democratic National Convention next week. He discussed key partnerships with state and local agencies in applying a layered approach to security at a press conference. "We will have mobile command vehicles positioned at strategic locations to coordinate communications across multiple law enforcement agencies to ensure that any vital tips or pieces of information do not slip through the cracks," he said. Ridge also said **there will be 24/7 surveillance of key convention facilities, as well as portable x-ray equipment to examine packages, as well as commercial vehicles and delivery trucks, entering these areas.** Trained homeland security personnel will augment the work of local law enforcement, record numbers of canine bomb teams will be utilized, and security will be increased at hotels to protect both the building and ventilation systems. Key transportation systems will be monitored and protected as well. Additional information is available here: <http://www.dhs.gov/dhspublic/display?content=3840>

Source: <http://www.dhs.gov/dhspublic/>

[[Return to top](#)]

Emergency Services Sector

31. *July 14, Disaster News Network* — **Fire lessons learned. The face of evacuation procedures might be changing as a result of lessons learned from last year's fierce wildfires in California.** Fourteen fires, from October 21 through November 4 last year, killed 24 people, destroyed 3,710 homes, and burned 750,000 acres. In some smaller communities, evacuation orders were issued via a helicopter equipped with a loudspeaker system, recalled Thomas Cova, a researcher from the University of Utah. In the future, instead of hearing an mandatory evacuation order, residents may be given the official choice: evacuate or shelter-in-place. **At**

least some research has shown that if residents are given the choice between evacuating and sheltering-in-place — that is, staying in their homes or staying in a community shelter — death tolls during wildfires are actually lower. One reason is because, if "we let people sort it out for themselves," they might avoid risky evacuations. Australia has already ceased all mandatory evacuation orders in favor of giving residents the choice of evacuating or sheltering in place. And in the U.S., Cova said, "sheltering in place is likely to be used in lieu of evacuating in an increasing number of cases. This is especially true in communities with defensible structures, or with good shelters."

Source: <http://www.disasternews.net/news/news.php?articleid=2301>

32. *July 13, KCRA (CA)* — **GPS technology helps track firefighters.** A Northern California fire department is using technology that helps dispatchers keep an eye on firefighters and their equipment. **Santa Rosa's fire department uses the same type of technology as global positioning systems, or GPS. It lets dispatchers watch a screen and keep track of every fire truck's every move.** For the past year, all 40 engines, cars, and ambulances in the department have been equipped with small disk-shaped antennas called automatic vehicle locators, or AVLs, which uses satellites in space to determine the vehicle's position within 10 feet. It then sends a signal back to headquarters and shows up as an icon on dispatchers' computer screens. **The department says the main reason for AVLs is to improve response time. Instead of simply calling out the crew whose station is nearest an incident, dispatchers can see if there might be an even closer crew passing nearby.**

Source: <http://www.thekcrachannel.com/news/3526147/detail.html>

[[Return to top](#)]

Information Technology and Telecommunications Sector

33. *July 15, The Chosun Ilbo (South Korea)* — **South Korean government, private sectors exposed to Chinese hacker attacks.** The National Intelligence Service (NIS) in South Korea confirmed Tuesday, July 13, that major government organizations and private sectors have been exposed to hacker attacks that came from China and declared the attack a "threat to national security." As a result, the NIS warned the public to protect their computers from hacking. **The NIS also said that based on their judgment, the attack was not carried out by individuals but involved an organization of some size,** they will collaborate with other government agencies such as the Foreign Ministry, Information and Communications Ministry, Defense Security Command, and National Police Agency to actively cope with it. **The NIS said that the two hacking programs, Peep Trojan and its variation Bacdoor Revacc, have broken into 211 computers in 10 government agencies.** Since the NIS announced on June 19 that a hacker attacked 116 computers, including 64 computers in the public sector and 52 computers in the private sector, an additional 162 computers have been attacked in some 20 days.

Source: <http://english.chosun.com/w21data/html/news/200407/200407130.036.html>

34. *July 13, Washington Post* — **Al Qaeda messages posted on U.S. server.** An Internet computer server operated by an Arkansas government agency was transformed last weekend into the online home of dozens of videos featuring Osama bin Laden, Islamic jihadist anthems and terrorist speeches. State government officials removed the files from a computer operated by the Arkansas Highway and Transportation Department shortly after they were discovered, a

government spokesman said. **The case highlights an increasing trend of hackers hijacking vulnerable Web servers for the purpose of advocating radical political and terrorist ideologies.** Links to the files were posted to a message board of a group called al Ansar. Arkansas Transportation Department spokesman Randy Ort confirmed that approximately 70 unauthorized files were posted on Sunday to a "File Transfer Protocol" (FTP) site that the agency operates for contractors. Ort would not describe the files, except to say that they were labeled "in a foreign language." Ort said that the FBI has confiscated the server where the files were located. FBI spokesman Joe Parris confirmed that the agency took the computers.
Source: http://www.washingtonpost.com/wp-dyn/articles/A47681-2004Jul_13.html

- 35. July 13, Government Computer News — Final E-Authentication architecture approved.** The General Services Administration (GSA) Monday, July 12, released the final piece to the E-Authentication puzzle. The Quicksilver project's executive board approved the final architecture for a federated portal. This final guideline ties together the administration policy on authentication levels and National Institute of Standards and Technology technical guidance. **The final architecture addresses authenticating end users to applications through a portal, the agency transaction or the credential service provider.** The portal will use Security Assertion Markup Language scheme to verify the identity of remote users accessing government systems. GSA also released the adopted scheme for the SAML architect profile and the interface specifications for the SAML profile. Additional information available here: <http://www.cio.gov/eauthentication/TechSuite.htm>
Source: http://www.gcn.com/vol1_no1/daily-updates/26561-1.html

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis			
<p>Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.</p> <p>US-CERT Operations Center Synopsis: Microsoft has released its July Security Updates. Two of these updates are of a critical nature and should be applied to vulnerable systems. For more information, see Microsoft's bulletin here.</p> <p style="text-align: center;">Current Port Attacks</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; padding: 5px;">Top 10 Target Ports</td> <td style="padding: 5px;"> 135 (epmap), 445 (microsoft-ds), 9898 (dabber), 5554 (sasser-ftp), 137 (netbios-ns), 1434 (ms-sql-m), 1433 (ms-sql-s), 3127 (mydoom), 1025 (blackjack), 22 (ssh) Source: http://isc.incidents.org/top10.html; Internet Storm Center </td> </tr> </table> <p style="font-size: small;">To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.</p> <p style="font-size: small;">Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it-isac.org/.</p>		Top 10 Target Ports	135 (epmap), 445 (microsoft-ds), 9898 (dabber), 5554 (sasser-ftp), 137 (netbios-ns), 1434 (ms-sql-m), 1433 (ms-sql-s), 3127 (mydoom), 1025 (blackjack), 22 (ssh) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
Top 10 Target Ports	135 (epmap), 445 (microsoft-ds), 9898 (dabber), 5554 (sasser-ftp), 137 (netbios-ns), 1434 (ms-sql-m), 1433 (ms-sql-s), 3127 (mydoom), 1025 (blackjack), 22 (ssh) Source: http://isc.incidents.org/top10.html ; Internet Storm Center		

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

36. *July 14, Associated Press* — **In Harrisburg, object found not to be a bomb. A suspicious item found outside the 11-story federal office building in downtown Harrisburg, PA, was detonated on the morning of Monday, July 13, though authorities later determined it was not a bomb.** Investigators who collected the blast debris concluded that the item did not have an igniter, Federal Bureau of Investigation (FBI) spokeswoman Jerri Williams said. "It could not have exploded on its own, or with an off-site detonator," she said. Several hundred people who had been evacuated were allowed to reenter the building about 2:30 p.m., and closed streets were reopened. U.S. Marshal Michael Regan said a delivery person first reported seeing the device on Court Street, an alley that runs behind the building. The federal building houses courtrooms, the U.S. Attorney's Office, a post office, and other federal offices.

Source: http://www.philly.com/mld/inquirer/news/local/states/pennsylvania/cities_neighborhoods/philadelphia/9147340.htm

37. *July 14, Associated Press* — **Police and firefighters have new computerized database.** Minneapolis, MN, city police officers and firefighters will soon be able to get a computer printout of the layout of downtown buildings before they arrive at the scene of an emergency. City public safety officials presented the beginning, and the promise, of a computer database of the largest downtown buildings on Tuesday, July 13. Public safety officials worked with downtown businesses to develop the program, called i-SITE. It has the layouts of four buildings online so far, and Target Corporation headquarters will be added soon, officials said. Interim Minneapolis Fire Chief Bonnie Bleskachek demonstrated the system on a laptop computer in a fire-truck command center. **The laptop showed a map indicating the locations of elevators and stairways, fire-hose connections, halls and utility shutoffs. The program also will tell emergency workers how many people work in specific buildings, what kinds of hazardous materials are inside and what emergency systems are in place.** About 90 downtown businesses have said they would like to participate in the program.

Source: http://wcco.com/localnews/local_story_196121019.html

38. *July 14, Associated Press* — **Suspected pipe bomb found in Thermopolis. A suspected pipe bomb found in Hot Springs State Park, WY, was safely detonated by police and caused the evacuation of part of the park.** Thermopolis, WY, Police Chief Jim Weisbeck said tourists spotted the suspicious looking device near a boat ramp in the park Tuesday morning, July 13. The device had three pieces of copper tubing that were capped and held together with duct tape, Weisbeck said. A portion of the park, including a nearby public swimming pool, was evacuated while a bomb disposal unit from Natrona County, WY, blew up the device. What is left of the device will be studied by the state crime lab to determine whether it was a pipe bomb, Weisbeck said. The Thermopolis incident comes less than a week after a suspected pipe bomb caused the evacuation of the Grand Teton National Park visitor's center.

Source: <http://www.casperstartribune.net/articles/2004/07/14/news/wyoming/8ebd09cc3e57327387256ed10058de16.txt>

[[Return to top](#)]

General Sector

39.

July 14, Reuters — **CIA's acting chief says threat highest since 9/11. The terrorist threat against the U.S. in the run-up to the November election is as serious as at any time since the September 11, 2001, attacks,** acting CIA Director John McLaughlin said on Tuesday, July 13. He said **the threats were not pinned specifically to the Democratic and Republican political conventions this summer but to the whole period before the November presidential election.** "It's related to this period during which the country is exercising its democracy, it's this period particularly in the run-up to the election, but it's always a mistake in the counterterrorism business to focus uniquely on a date," McLaughlin said. The attackers would strike when they are ready and not because of a specific date, he said. Senate Intelligence Committee Chairman Pat Roberts earlier on Tuesday told reporters that "the chatter and the texture of the chatter is the highest it's been since 9/11." Chatter refers to communications among terrorism suspects. Department of Homeland Security Secretary Tom Ridge renewed public warnings last week of possible attacks by al Qaeda in the U.S. this year, but offered no details and said there were no plans to raise the terror threat level.

Source: <http://news.myway.com/top/article/id/387144|top|07-13-2004:: 20:47|reuters.html>

[[Return to top](#)]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Alerts](#) – Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues.

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.